

REMARKS

The application has been carefully reviewed in light of the Office Action. Claims 1 to 104 and 122 to 140 are pending in the application, of which Claims 1, 2, 13, 16, 17, 29, 32, 33, 45, 48, 49, 61, 64, 65, 76, 79, 80, 92, 95, 96, 122, 125, 126 and 138 are the independent claims. Reconsideration and further examination are respectfully requested.

Turning to the art rejection, Claims 1, 16, 32, 48, 64, 79, 95 and 126 were rejected under 35 U.S.C. § 103(a) over Applied Cryptography (Schneier); Claims 2 to 7, 10 to 13, 17 to 24, 27 to 29, 33 to 38, 42 to 45, 49 to 55, 59 to 61, 65 to 70, 74 to 76, 80 to 86, 90 to 92, 96 to 101, 122, 126 to 132 and 136 to 138 were rejected under § 103(a) over U.S. Patent No. 6,560,581 (Fox) in view of Schneier; and Claims 8 to 10, 14, 15, 24 to 26, 30, 31, 29 to 41, 46, 47, 56 to 58, 62, 63, 71 to 73, 77, 78, 87 to 89, 93, 94, 102 to 104, 123, 124, 133 to 135, 139 and 140 were rejected under § 103(a) over Fox in view of Schneier, and further in view of U.S. Patent No. 6,243,466 (Young). Reconsideration and withdrawal of these rejections are respectfully requested.

With respect to specific claim language, independent Claim 1 is directed to a method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient. The method includes an encrypting step of twice encrypting the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image. The

method also includes a transmitting step of transmitting the twice-encrypted data to the intended image output device.

The Examiner stated in the Office Action that it would have been obvious to one of ordinary skill in the art to combine the method of double encryption as disclosed by Schneier with the method of using asymmetric key encryption as disclosed by Schneier. However, Schneier is not seen to disclose the feature of Claim 1 and is not seen to disclose any suggestion or motivation to combine the above-mentioned methods.

Schneier is seen to teach that double encryption is performed so that the encrypted data is not decoded easily. Further, Schneier is seen to disclose the method of using asymmetric key encryption, but Schneier is not seen to disclose that the asymmetric key is used when data is double-encrypted. Therefore, Schneier is only seen to disclose the method of double encryption and the separate method of using asymmetric key encryption.

In contrast, Claim 1 of the present invention describes a method for twice encrypting the data using two different sets of asymmetric keys, a first key being a public key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and a second key being a public key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image.

According to the present invention, in order to decrypt a message, both the private key of the intended image output device and the private key of the intended recipient of the image output device are required. The encryption method of the present invention ensures that only the presence of the intended recipient at the intended image

output device will result in decryption of the data. Schneier is not seen to disclose or suggest such a combination of decryption features.

Based on the foregoing remarks, Applicants respectfully submit that Schneier is not seen to render obvious the invention of independent Claim 1. Independent Claim 1 is therefore believed to be in condition for allowance. In addition, independent Claims 16, 32, 48, 64, 79, 95 and 126 contain substantially similar features as those of independent Claim 1, and are therefore also believed to be in condition for allowance for at least the same reasons as discussed above with respect to independent Claim 1.

Independent Claim 2 is directed to a method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient. The method includes a first encrypting step of encrypting the data using a first key, a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image, and a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

The applied art, namely Schneier and Fox, is not seen to disclose or suggest the foregoing features of independent Claim 2. In particular, Schneier is seen to disclose a triple key encryption method for encrypting a block of data three times using three different sets of symmetric keys to strengthen the encryption. However, as discussed above with respect to independent Claim 1, nowhere is Schneier seen to disclose or suggest the use of

public/private key for secure data or key encryption in the aforementioned triple key encryption method. In addition, the triple key encryption method of Schneier cannot be seen to provide additional security for secure transmission of data to an intended image output device.

In this regard, Fox is not seen to remedy the foregoing deficiencies of Schneier with respect to independent Claim 2. Fox is seen to disclose a method for encrypting a document using a symmetric encryption key, and then encrypting that key with a public key of the merchant that is intended to receive the document (Fox, columns 61 to 65). As stated in the Office Action, Fox does not disclose an encryption method using a set of asymmetric keys as disclosed in independent Claim 2. Although the method disclosed in Fox can assure that only the intended recipient can decrypt the symmetric key by using its private key, Fox is not seen anywhere to provide secure transmission of data to an intended image output device. The encryption method of the present invention of Claim 2 ensures that only the presence of the intended recipient at the intended image output device will be able to decrypt the data. On the contrary, unlike the present invention of Claim 2, Fox's encryption method allows the intended recipient to decrypt the document at any location, and does not require that the intended recipient to be present at the intended image output device for decryption to occur, as in the present invention.

Based on the foregoing, Applicants respectfully submit that Schneier and Fox, either alone or in combination, are not seen to render obvious the invention of independent Claim 2 because those references are not seen to teach the combination of features of independent Claim 2. Independent Claim 2 is therefore believed to be in condition for allowance, and such action is respectfully requested. In addition, Claims 13, 17, 29, 33, 45, 49, 61, 65, 76, 80, 92, 96, 122, 125 and 138 are independent claims

containing substantially similar features as those described in independent Claim 2, and are therefore also believed to be in condition for allowance for at least the same reasons as those discussed above with respect to independent Claim 2.

The other pending claims in this application are each dependent from the independent claims discussed above and are therefore believed patentable for the same reasons. Because each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration of each on its own merits is respectfully requested.

In view of the foregoing remarks, the entire application is believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Applicants' undersigned attorney may be reached in our Costa Mesa, CA office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

  
\_\_\_\_\_  
Attorney for Applicants

Registration No. 40,595

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-2200  
Facsimile: (212) 218-2200

CA\_MAIN 75316 v 1